

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with 18 email addresses listed in Attachment [A] that
is stored at premises controlled by
Google, Inc.
1600 Amphitheatre Parkway, Mountain View, CA 94043

Case No. 2:18-mj-776

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. 1343
18 U.S.C. 371
18 U.S.C. 1956

Wire Fraud
Conspiracy
Money Laundering

Offense Description

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Richard Gourley, Special Agent, IRS-CI

Printed name and title

Sworn to before me and signed in my presence.

Date:

10-12-18

Judge's signature

City and state: Columbus, Ohio

CHELSEY M. VASCURA, United States Magistrate Judge

Printed name and title

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Richard Gourley, Special Agent, Department of the Treasury, IRS Criminal Investigation, being duly sworn, depose and say that I am one of the Lead Investigators in this investigation. I have consulted with the other Lead Investigators regarding this investigation and have probable cause to believe the following is true, based on the investigation to date:

INTRODUCTION

1. I am a Special Agent with the Internal Revenue Service, Criminal Investigation Division (IRS-CID) and have been so employed since July 27, 2006. I received Criminal Investigator Training and Special Agent Investigator Training at the Federal Law Enforcement Training Center in Glynco, Georgia. This training included the laws of search and seizure, use of search warrants in an investigation of tax-related crimes, accounting principles, tax and financial investigative techniques, and investigation of Bank Secrecy Act (BSA) related matters. In addition, I have received specialized training in money laundering and asset forfeiture. My responsibilities as a Special Agent include the investigation of potential criminal violations of the Internal Revenue Code, as covered under Title 26 of the United States Code, and additional violations of federal law found under Title 18 and Title 31 of the United States Code. I have participated in the execution of search warrants and arrests related to the above-referenced offenses.

a) Throughout this affidavit, reference to “investigators” specifically refers to criminal investigators;

2. Based on our ongoing investigation, your affiant believes that there is probable cause to find that Terry Boutwell (Boutwell), Tiffany A. Strobl (Strobl), and others, are engaged in a scheme to defraud online consumers by falsely offering for sale motor vehicles through an online marketplace and further evidence and instrumentalities of this fraud are located in electronic format on the computer systems and servers of Google, Inc. in multiple accounts described below.

PURPOSE OF AFFIDAVIT

3. Your affiant submits there is probable cause to believe that evidence of crime, namely criminal violations of the federal criminal code (Title 18), including § 1343 (wire fraud), § 371 (conspiracy to commit an offense), and § 1956 (money laundering) are located in

electronic format on the computer systems and servers of Google, Inc. in the following email accounts:

jimmypang44@gmail.com
timmywang9898@gmail.com
timlee5454@gmail.com

denise.raymond67@gmail.com
galeauea@gmail.com
cardsg4@gmail.com
payme0181@gmail.com
bshireley@gmail.com
holly.toner83@gmail.com
vanessawilliams870@gmail.com
toddrichman1@gmail.com
prepaidcustomer18@gmail.com
moderneffectscalls@gmail.com
elegantbeautyproductsmia@gmail.com
moderneffectsdetroit@gmail.com
godaffiliated@gmail.com
reneeorb@gmail.com
s.g.chickey@sudenllinks.net

4. Because this affidavit is offered for the limited purpose of establishing probable cause in support of this warrant, it does not set forth all facts known to this investigation.
5. Your affiant anticipates executing this warrant under the Stored Communications Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) described in Attachment B, Section I. Upon receipt of the information described in Attachment B, Section I, government-authorized persons will review that information to locate the items described in Attachment B, Section II.

LOCATION TO BE SEARCHED

See Attachment A.

ITEMS TO BE SEIZED

See Attachment B.

INVESTIGATIVE SUMMARY

6. Beginning in or before April 2015, individuals known and unknown to this investigation initiated a scheme to defraud online consumers by falsely offering for sale various motor vehicles through an online marketplace. Victims are enticed by competitive pricing and the offer of a "buyer protection plan" through eBay, whereby victims are instructed to wire funds for their purchase to what they believed is an eBay escrow account where the funds would be held until the victim had received their purchase. In reality, there are no motor vehicles to be sold and the false escrow accounts are held by individuals who have no affiliation with eBay or eBay Motors and who promptly withdraw the majority of funds received in cash, and in some cases used funds to purchase virtual currency (Bitcoins).
7. Hundreds of alleged victims throughout the United States and numerous false escrow accounts have been identified. These accounts have received in excess of \$5 million to date, all of which is believed to be derived from the fraud scheme.
8. As part of the fraud scheme, multiple business entities have been established in various states, all of which make reference to or are derivative of "eBay Buyer Protection;" these entities include EEBPA LLC, EEBP LLC, EBPA LLC, EBMP Associates, EBMP Services, Empire Builder Productions LLC, Enison Business Protection Advisors LLC, Ecommerce Business Protocol Architects, Evil Boy Productions, Elegant Beauty Products LLC, Extraordinary Business Products & Applications LLC, Enterprise Business Planning, and Easy Business Partners, among others.
9. In or around September 2015 Terry Boutwell was arrested; pursuant to this arrest multiple electronic devices were seized and later searched pursuant to a federal search warrant in the Northern District of Ohio.
10. In or around April 2016 Tiffany Strobl was arrested; pursuant to this arrest multiple electronic devices were seized and later searched pursuant to a federal search warrant in the Southern District of Ohio.
11. In or around February 2017 Tiffany Strobl was again arrested; pursuant to this arrest multiple electronic devices were seized and later searched pursuant to a federal search warrant in the Southern District of Florida.
12. In or around May 2017 a search warrant was executed in the Southern District of Ohio on multiple Google email accounts including **timmywang9898@gmail.com** and **jimmylang9898@gmail.com**.

13. In or around December 2017 a search warrant was executed in the Southern District of Ohio on multiple Google email accounts including ecommercebusinesspioneers@gmail.com; farmerjohn0915@gmail.com, elmasboutiquepa@gmail.com, jimmypang44@gmail.com and timlee5454@gmail.com.

PROBABLE CAUSE

14. The information in this affidavit is a compilation of information developed during the ongoing criminal investigation that started in 2015 of the above-described violations. The investigation has been conducted by investigators of the IRS-CI, FBI, U.S. Postal Inspectors Service, and U.S. Secret Service, along with multiple state and local investigative agencies. Investigators' knowledge is derived from their own personal observations and from a variety of credible sources, including witness interviews; reviews of bank records, public records, and documents from individuals and businesses; and information provided to them by other law enforcement and regulatory personnel with the IRS-CI, the FBI, the U.S. Secret Service, U.S. Postal Inspectors Service, and local law enforcement officials. This affidavit is intended to show that there is sufficient probable cause for the requested search warrant and does not purport to set forth all investigators' knowledge of the investigation into this matter. The investigation undertaken by the investigators involves conduct in multiple federal judicial districts, including the Southern District of Ohio, Northern District of Ohio, District of Maryland, Southern District of New York, Southern District of Florida, Eastern District of Michigan, Southern District of Alabama, and District of Columbia.
15. On or about April 6, 2015, Boutwell established a bank account with PNC Bank held in the name EEBPA, LLC, ending with account #3485. Boutwell received five (5) wires from individuals into this account totaling \$45,700. Boutwell made cash withdrawals from this account totaling \$45,600.
- a) One of the wires received into this account was from an individual hereinafter referred to as Terry Boutwell Victim #1 (TBV1). On or about July 2, 2015, TBV1 filed a police report with the Butler Village, Ohio Police Department, alleging to be the victim of a fraud scheme. TBV1 stated that in May 2015, TBV1 attempted to purchase an all-terrain vehicle on Craigslist.com. TBV1 believed to be purchasing the vehicle from an individual named Scott Brownell who represented that he was U.S. Military personnel located in Alaska. Scott Brownell instructed TBV1 that the sale would take place using eBay's Buyer Protection Program and TBV1 was subsequently in contact with an individual named "Alex" who represented to be employed by eBay Motors. TBV1 received an email with eBay Motors letterhead detailing the transaction parties and was instructed to wire funds to the EEBPA account held by Boutwell at PNC Bank. TBV1 wired the funds but never received the all-terrain vehicle purchased and after contacting

eBay, TBV1 learned they were the victim of a scam;

- b) A second wire received into this account was from an individual hereinafter referred to as TB Victim #2 (TBV2). On or about May 19, 2015, TBV2 filed a police report alleging to be the victim of a fraud scheme. TBV2 stated in May 2015, TBV2 attempted to purchase a motorcycle on Craigslist.com. TBV2 believed to be purchasing the vehicle from an individual named Ashley Robbins who represented she was U.S. Military personnel being re-located to Alaska. Ashley Robbins instructed TBV2 that the sale would take place using eBay. TBV2 was instructed to call 855-915-EBAY and did so, speaking with someone TBV2 recalled as being possibly named "Alex" who instructed TBV2 on where to send the wire payment; TBV2 received an email with eBay Motors letterhead detailing the transaction parties and was instructed to wire funds for the purchase to the EEBPA account held by Boutwell at PNC Bank. TBV2 never received the vehicle and contacted eBay concerning the purchase and was told the eBay account in question was fake;

16. In or around June 2015, Tiffany Strobl (Strobl) opened two accounts with Citibank in the name of EBPA, LLC, ending with account #9965 and account #9973.

- a) The listed address of EBPA, LLC is 2200 Pennsylvania Ave NW 4 FL, Washington, D.C. 20037. This address is known to be rentable office space operated by Regus. Included with Strobl's account opening documents is an IRS Form W-9 Request for Taxpayer Identification Number and Certification. Strobl lists her address on this form as 1723 Richmond Avenue, Columbus, Ohio. Your affiant is aware that Strobl rented an apartment at this address from on or about May 31, 2014 through her eviction on January 20, 2016;
- b) Strobl received eleven (11) wires from individuals into this account totaling \$101,500. Strobl made cash withdrawals from these accounts totaling approximately \$93,000;

17. Records obtained from JPMorgan Chase Bank show in April 2015 Boutwell opened JPMorgan Chase bank account ending in #9953 in the name of EEBPA LLC with a listed business address of 1723 Richmond Ave Apt 1, Columbus, OH 43203. This account received approximately \$231,580 in cash deposits between April 2015 and September 2015 and received approximately \$149,295 in wire transfers from an account held in the name EBPA LLC at TD Bank.

18. Records obtained from TD Bank show that in June 2015, Strobl opened two accounts, ending in #1500 and #1518 both in the name EBPA LLC; the accounts were funded primarily by wire transfers and cash deposits and also show subsequent wire transfers to the JPMorgan Chase Bank account ending in #9953 controlled by Boutwell listed above.

19. Boutwell was arrested in September 2015 and multiple electronic devices were seized from Boutwell at that time. These electronic devices included a LG H345 cellphone Android ID #4fd5fdb7e4441958 (Boutwell LG) and a Samsung Galaxy S5 cellphone Android ID#25deb4a960f5cf95 (Boutwell Samsung). A federal search warrant was authorized and executed in the Northern District of Ohio for these electronic devices, among other items. The devices contained multiple email communications with co-conspirators regarding the fraud scheme.
20. In or around April 2016, Strobl was arrested in Bloomfield Township, Michigan and multiple electronic devices were seized from Strobl at that time. Among other items, investigators located a Samsung Galaxy S4 cellphone IMEI #990005910004564 (Strobl Samsung1) and a Samsung Galaxy S4 cellphone IMEI #990004831912393 (Strobl Samsung). A federal search warrant was authorized and executed for these devices as well. The devices contained multiple email communications with co-conspirators regarding the fraud scheme.
21. Documents in Strobl's possession at the time of her arrest also included debit/credit cards bearing the name Melissa Ramsey; Melissa Ramsey is associated with the fraud scheme as follows:
 - a) Documentation on file with the State of Virginia State Corporation Commission names Melissa Ramsey as the organizer of Ecommerce Business Protocol Associates LLC with a principal address of 211 North Union Street Suite 100, Alexandria, Virginia 22314;
 - b) Documentation on file with the State of Michigan Department of Licensing and Regulatory Affairs names Melissa Ramsey as the sole member of Ecommerce Business Protocol Architects LLC with a principal address of 2000 Town Center Suite 1900, Southfield, Michigan 48075;
 - c) Information obtained from KeyBank states that Melissa Ramsey is the authorized signer for two accounts held in the name Ecommerce Business Protocol Architects;
 - i. On or about April 18, 2016, one of these accounts received a wire totaling \$15,300 from an individual hereinafter referred to as Ramsey Victim #1 (RV1). RV1 stated they were interested in purchasing a recreational vehicle and found an ad on Craigslist. RV1 contacted Rebeca Dawson via email about the sale and was told that Rebeca Dawson and her husband were moving to Canada and needed to sell the vehicle quickly; the sale would take place through eBay and the vehicle was already at the shipping yard. RV1 agreed to purchase the vehicle at a price of \$15,300. RV1 was told to send payment to eBay via wire and the funds would be held until RV1 received the vehicle. RV1 would have seven days to decide to keep the

vehicle and if unsatisfied Rebeca Dawson would pay the shipping charges;

- ii. RV1 was instructed to call Karen Burke with eBay Finance Department outside the bank before sending the wire for instructions on where to send the wire. RV1 was also instructed to call Karen Burke after the wire was sent;
 - iii. RV1 never received the vehicle in question; RV1 attempted to contact Rebeca Dawson and Karen Burke but has not had any further contact with either individual. RV1 filed a police report detailing the activity;
- e) On or about October 6, 2016 investigators interviewed Melissa Ramsey. Ramsey stated:
- i. Ramsey got involved with what she believed was a bitcoin business through Strobl;
 - ii. Strobl explained to Ramsey that Ramsey would open bank accounts and receive deposits from individuals purchasing bitcoins. Ramsey was directed to withdraw these funds in cash and turn the cash over to Strobl;
 - iii. Strobl told Ramsey the cash was going to someone named "Bob;"
 - iv. Ramsey stated all of the individuals involved in the business have nicknames; Ramsey's nickname was "Rambo" and Strobl's nickname was "Ghost;"

22. Documents in Strobl's possession at the time of her arrest include debit/credit cards bearing the name Kaylee Sue Leininger; Kaylee Sue Leininger is associated with the fraud scheme as follows:

- a) Information obtained from Comerica Bank states that Kaylee Sue Leininger is the signer for two accounts held in the name Enison Business Protection Advisors. The listed address for these accounts is 100 Crescent Court 7th Floor, Dallas, Texas 75201; a Google search of this address shows it is a Regus office space;
- b) Records obtained from Bank of Texas show Kaylee Sue Leininger opened two accounts held in the name Enison Business Protection Advisors LLC. These accounts received one wire transfer totaling approximately \$9,000.
- c) Records obtained from Woodforest National Bank show Kaylee Sue Leininger opened two accounts held in the name Enison Business Protection Advisors LLC. These accounts received seven wire transfers totaling approximately \$78,750.
- d) On or about October 27, 2016 investigators interviewed Kaylee Sue Leininger. Leininger

stated:

- i. Leininger was recruited by a friend to work in a job involving bitcoins and traveled to Atlanta, GA where she was introduced to Strobl. Leininger traveled to Dallas, TX with Strobl and was directed to open multiple bank accounts;
- ii. Accounts opened by Leininger began receiving deposits which Leininger was told were for bitcoin purchases. Leininger was directed to withdraw cash from these accounts and turn it over to Strobl or the friend that recruited her;
- iii. Leininger never purchased or sold any bitcoins; Strobl gave Leininger an online class about bitcoins;
- iv. Leininger was told if she quit someone named "Bob" would be after her;

24. The email addresses **timmywang9898@gmail.com** is known to be used in furtherance of the fraud scheme:

- a) As referenced above, Boutwell was arrested in September 2015 and multiple electronic devices were seized from Boutwell at that time. These electronic devices included a Samsung Galaxy S5 cellphone (Boutwell Samsung) and LG H345 cellphone (Boutwell LG).
- b) Multiple email communications pertaining to the scheme were located on the Boutwell Samsung including:
 - i. On or about June 8, 2015, an email was sent from **apriltemp042015@gmail.com** to **timmywang9898@gmail.com** with the subject line "Ebpa inc file status;"
 - ii. On or about August 18, 2015, an email was sent from **timmywang9898@gmail.com** to **apriltemp042015@gmail.com** with the subject line "An0n Tuesday Edition" which contained in the body of the email various computations including "total owed to crew" and multiple dollar amounts including "85% of Tuesday's \$9500 into Ghost's 5/3rd." Bank records obtained from Fifth/Third bank for an account ending in #1295 show this account was opened in the name EBPA LLC and the sole accountholder is Tiffany Strobl; On or about August 18, 2015, a wire deposit of \$9,500 was received into this account;
- c) Multiple email communications pertaining to the scheme were located on the Boutwell LG including:

- i. On or about May 5, 2015, an email from **timmywang9898@gmail.com** to **apriltemp042015@gmail.com** was forwarded to **witchdocda@gmail.com**; the body of the email contained bank account information for a bitcoin buyer/seller located in Santa Monica, CA;
 - ii. On or about August 5, 2015, an email was sent from **apriltemp042015@gmail.com** to **timmywang9898@gmail.com** with the subject line "Caspers WF" which contained in the body of the email address and bank account information for a business named EMBP SERVICES LLC;
 - iii. On or about August 17, 2015, an email was sent from **apriltemp042015@gmail.com** to **timmywang9898@gmail.com** with the subject line "Starlett Citizens" which contained in the body of the email bank account information for a business named EEBPA LLC;
25. The email address **jimmypang44@gmail.com** is known to be used in furtherance of the fraud scheme:
- a) In or around May 2017 a federal search warrant was authorized and executed in the Southern District of Ohio for various Google email accounts including **thomeyjessica99@gmail.com**, **timmywang9898@gmail.com** and **jimmylang9898@gmail.com**; a review of evidence received from the execution of this warrant yielded the following:
 - i. An email received by **timmywang9898@gmail.com** on or about November 9, 2016 was a forwarded email message from **jimmypang44@gmail.com**; this email was from **customer@freedomvoice.com** and detailed the customer ID 292929, a phone number, and username which was also **jimmypang44@gmail.com**; the phone number established contains the numbers "3229" which match the letters E-B-A-Y on a telephone dial pad;
 - FreedomVoice was served a subpoena for this account among others; records obtained from FreedomVoice show that customer ID 292929 between 11/9/2016 and 12/16/2016 received approximately 254 telephone calls answered both by "user" and by "voicemail;"
 - b) In or around December 2017 a federal search warrant was authorized and executed in the Southern District of Ohio for various Google email accounts including **jimmypang44@gmail.com**. Among the evidence identified in that email account were the following emails:

- i. Multiple emails sent from the email address **jimmypang44@gmail.com** to the email address **invoice67@gmail.com** with subject lines referencing eBay Buyer Protection and Order ID numbers, and which contained in the body of the emails vehicle sales data including buyer, seller, vehicle identifiers, and cost.
- ii. Multiple emails from the email address **jimmypang44@gmail.com** to the email address **timlee5454@gmail.com** with the subject lines referencing eBay Buyer Protection and Order ID numbers, and which contained in the body of the emails vehicle sales data including buyer, sell, vehicle identifiers, and cost.
- iii. An email dated on or about January 17, 2017 sent from the email address **jimmypang44@gmail.com** to a Yahoo, Inc. email address with the subject line “Hey – Working?” and which contained in the body the message “Hi, I was Terry / Anon’s boss. I was the one that had all the leads for the ebay stuff. Are you guys still working? Would love to connect with you guys. Let me know.”

26. The email address **timlee5454@gmail.com** is known to be used in furtherance of the fraud scheme:

- a) In or around March 2017 through April 2017 multiple emails were sent from **timmywang9898@gmail.com** to **timlee5454@gmail.com** including:
 - i. On or about March 31, 2017 an email was sent with the subject line “ad” which in the body contained a description for a 2007 GMC Sierra Denali;
 - ii. On or about April 14, 2017 an email was sent with the subject line “Script” which in the body contained detailed instructions for describing “ebay financial services” and included the greeting “EBAY FINANCIAL SERICES, THIS IS ALEX, HOW CAN I HELP YOU TODAY;” the script also contains answers to provide customers who ask if the sale is a scam;
 - iii. On or about April 25, 2017 an email was sent with the subject line “buyer info” which in the body contained five individual names with corresponding phone numbers and email addresses;
- b) In or around February 2017 through April 2017 **timlee5454@gmail.com** also sent multiple emails to **timmywang9898@gmail.com** including:
 - i. On or about March 16, 2017 an email was sent with the subject line “an0n” and in the body stated “we can use this email;”

- ii. On or about February 27, 2017 an email with the subject “Funds – Invitation to edit” which contained in the body an invitation to edit a document through Google Docs;
 - c) As referenced earlier in this document multiple emails were sent from the email address **jimmytang44@gmail.com** to the email address **timlee5454@gmail.com** with the subject lines referencing eBay Buyer Protection and Order ID numbers, and which contained in the body of the emails vehicle sales data including buyer, sell, vehicle identifiers, and cost.
27. Many of the email addresses used in this scheme have maintained incoming and/or outgoing emails for long periods. For example, the email address **farmerjohn0915@gmail.com** which was obtained in the previous search warrant in or around December 2017 contained emails dating from at least September 2015 through December 2017; the email address **timmywang9898@gmail.com** which was obtained in the previous search warrant in or around May 2017 contained emails dating from at least August 2016 through May 2017 and the email address **timlee5454@gmail.com** which was obtained in the previous search warrant in or around December 2017 contained emails dating from at least February 2017 through December 2017;
28. Your Affiant knows the fraud scheme continues to the present day with victim complaints matching the style and methods of this fraud scheme being submitted to law enforcement as recently as September 25, 2018;

THE EMAIL ACCOUNTS

***jimmytang44@gmail.com AND timlee5454@gmail.com AND
timmywang9898@gmail.com***

29. Records obtained from Google, Inc. show the email address **jimmytang44@gmail.com** as created on or about June 21, 2016 and the account was logged into as recently as on or about July 5, 2018;
30. Records obtained from Google, Inc. show the email address **timlee5454@gmail.com** was created on or about February 19, 2017 and the account was logged into as recently as on or about March 15, 2018; the listed recovery address for this email account is **prepaidcustomer18@gmail.com**;
31. Records obtained from Google, Inc. show the email address **timmywang9898@gmail.com** was created on or about March 14, 2014;

32. In or around May 2017 and in or around December 2017 federal search warrants were authorized and executed for various Google email accounts including **timmywang9898@gmail.com** (May 2017), **jimmypang44@gmail.com** (December 2017) and **timlee5454@gmail.com** (December 2017). These accounts communicated with each other and multiple other email addresses as described earlier in this document, and as follows:
33. From in or around August 2016 through September 2016, multiple emails were sent from **timmywang9898@gmail.com** to the email address **invoice67@gmail.com** including:
- a) An email dated on or about August 25, 2016 with the subject line “buyer info” that included a list of six individual names with corresponding email addresses and telephone numbers;
 - b) An email dated on or about August 23, 2016 with the subject line “DROPS” that included in the body of the email the name EBFS with corresponding address and bank account number, and the name EEFS with corresponding address and bank account number;
34. In or around March 2017 through April 2017, multiple emails were sent from **timmywang9898@gmail.com** to **timlee5454@gmail.com** as detailed more fully earlier in this document;
35. In or around February 2017 through April 2017, **timlee5454@gmail.com** also sent multiple emails to **timmywang9898@gmail.com** as detailed more fully earlier in this document;
36. On or about September 23, 2016, an email was sent from **timmywang9898@gmail.com** to **newemail201520152015@gmail.com** with the subject line “Call Bob ASAP” which contained no text in the body of the email.
- a) Multiple individuals interviewed by investigators in this investigation stated they spoke with someone named “Bob” who appeared to be acting in a leader/organizer capacity;
37. Records were obtained via search warrant for the email address **timmywang9898@gmail.com** through May 2017 and records were obtained for the email address **timlee5454@gmail.com** through December 2017; Those records for **timlee5454@gmail.com** revealed communications between **timmywang9898@gmail.com** and **timlee5454@gmail.com** for the period after May 2017 up to in or around November 2017 including numerous emails with links to **privnote.com** messages; your Affiant knows **privnote.com** to be a website that offers users the ability to send free confidential and self-destructing messages via email;

38. Records obtained for the email address **jimmypang44@gmail.com** also show communications between **jimmypang44@gmail.com** and **timmywang9898@gmail.com** for the period in or around June 2017;

denise.raymond67@gmail.com

39. Records obtained from Google, Inc. show the email address **denise.raymond67@gmail.com** was created on or about February 14, 2017 and the account was logged into as recently as on or about July 6, 2018;

40. The email address **denise.raymond67@gmail.com** sent two emails to **jimmypang44@gmail.com** in or around June 2017 as follows:

- a) An email dated on or about June 13, 2017 with the subject line “text 1” that contains in the body an email to someone named “Norman” and which details the sales and shipping process for a 2007 Airstream Safari SE and states “The financial part will be managed by eBay...” This email was forwarded from **jimmypang44@gmail.com** to **timmywang9898@gmail.com** on or about June 19, 2017;
- b) An email dated on or about June 13, 2017 with the subject line “text 2” that contains further instructions to “Norman” and again references eBay stating “You will need to make the payment to eBay...” This email was also forwarded from **jimmypang44@gmail.com** to **timmywang9898@gmail.com** on or about June 19, 2017;

galeaua@gmail.com

41. Records obtained from Google, Inc. show the email address **galeau@gmail.com** was created on or about March 7, 2008 and the account was logged into as recently as on or about August 6, 2016;

42. The email address **galeaua@gmail.com** sent multiple emails to the email address **jimmypang44@gmail.com** including the following:

- a) An email dated on or about October 13, 2016 with the subject line “FWD Order ID#: 32291680252 which contained in the body details for the sale of a 2010 4WD John Deere Tractor being sold by “Vanessa Williams” to an individual hereinafter referred to as Person - DT and is identified by eBay Buyer Protection – Order ID#: 32291680252.
- b) An email dated on or about October 27, 2016 with a subject line referencing Person – DT which contained in the body an image of a wire transaction receipt dated October 18, 2016 from Bank of America to a JPMorgan Chase Bank account ending in #1119.

- i. Bank records obtained from JPMorgan Chase Bank show the account ending in #1119 is an account opened in the name EVER BOND FABRIC SERVICE and this account received a wire transfer from Person - DT on or about October 18, 2016 totaling \$10,800.

cardsg4@gmail.com

43. Records obtained from Google, Inc. show the email address **cardsg4@gmail.com** was created on or about February 12, 2017;
44. The email address **cardsg4@gmail.com** sent at least two emails to the email address **jimmypang44@gmail.com** in or around February 2017 as follows:
 - a) An email dated on or about February 13, 2017 with the subject line "GIFT CARDS – Invitation to edit" and contained in the body a link to a Google Sheets file for editing.
 - b) An email dated on or about February 14, 2017 with the subject line "Carlos Walmart Sheet – Invitation to edit" and contained in the body a link to a Google Sheets file for editing.
- i. In or around February 2017 Tiffany Strobl was arrested in Dania Beach, FL. Among the items in her possession was a Samsung cellular phone. A search warrant was obtained for that phone which contained the following evidence:
 - A text message from a phone number labeled with the name "Carlos Gc" dated on or about February 14, 2017 stating "Hey ghost this is carlos, when would be a good time to talk about the Wal-Mart operation."
 - A text message to "Carlos Gc" dated on or about February 14, 2017 stating "Hey can I get your email so I can give the invite for google docs"

payme0181@gmail.com

45. Records obtained from Google, Inc. show the email address **payme0181@gmail.com** was created on or about January 29, 2017 and was logged into as recently as on or about February 2, 2017;
46. The email address **payme0181@gmail.com** received at least one email from the email address **timmywang9898@gmail.com** as follows:

- a) An email dated on or about January 29, 2017 with the subject line “Call me when you can” that contained in the body the message “Hey you, call me asap”;

47. The email address **payme0181@gmail.com** sent multiple emails to the email address **jimmypang44@gmail.com** including the following:

- a) An email dated on or about February 16, 2017 with the subject line “Log on for BBT” that contained in the body what appears to be a username, password, and three security questions with corresponding answers;
- b) An email dated on or about January 29, 2017 with the subject line “phone scrip” that contained in the body a lengthy narrative about “EBAY FINANCIAL SERVICES” and answers to customer questions about the service;

bshireley@gmail.com

48. Records obtained from Google, Inc. show the email address **bshireley@gmail.com** was created on or about September 13, 2016 and was logged into as recently as on or about October 3, 2016;

49. The email address **bshireley@gmail.com** sent multiple emails to the email address **jimmypang44@gmail.com** including the following:

- a) An email dated on or about September 14, 2016 with the subject line “Tex 1 (1)” which contained in the body the description of a 1975 Volkswagen Bus for sale including reference to the seller having “been transferred to Elmendorf AFB”;
- b) An email dated on or about September 14, 2016 with the subject line “Text 3 (1)” which contained in the body the line “Let me explain to you how the entire process thru eBay works:” and seven bullet points explaining a purchase process;

holly.toner83@gmail.com

50. Records obtained from Google, Inc. show the email address **holly.toner83@gmail.com** was created on or about June 30, 2016 and was logged into as recently as April 19, 2018;

51. The email address **holly.toner83@gmail.com** received at least one email from the email address **jimmypang44@gmail.com** as follows:

- a) An email dated on or about January 18, 2017 with the subject line “I made your invoice” that contained in the body the message “Come online to get it”;

vanessawilliams870@gmail.com

52. Records obtained from Google, Inc. show the email address **vanessawilliams870@gmail.com** was created on or about September 14, 2016 and was logged into as recently as on or about February 10, 2017;

53. The email address **vanessawilliams870@gmail.com** sent at least one email to the email address **jimmypang44@gmail.com** as follows:

- a) An email dated on or about October 21, 2016 with the subject line “Fwd: Fwd: Your Same Day wire transfer was successfully sent” that contained in the body a forwarded email message from Bank of America detailing a wire transfer totaling \$10,800 to a JPMorgan Chase Bank account;

toddreichman1@gmail.com

54. Records obtained from Google, Inc. show the email address **toddreichman1@gmail.com** was created on or about November 23, 2016 and was logged into as recently as on or about July 1, 2017;

55. The email address **toddreichman1@gmail.com** received at least one email to the email addresses **jimmypang44@gmail.com** as follows:

- a) An email dated on or about January 31, 2017 with the subject line “Script” that contained a lengthy narrative about “EBAY FINANCIAL SERVICES” and answers to customer questions about the service; this email appears to be the same or similar to the email sent from **payme0181@gmail.com** to **jimmypang44@gmail.com** described earlier;

prepaidcustomer18@gmail.com

56. Records obtained from Google, Inc. show the email address **prepaidcustomer18@gmail.com** was created on or about June 7, 2016 and was logged into as recently as on or about July 12, 2018;

57. The email address **prepaidcustomer18@gmail.com** sent multiple emails to the email address **timlee5454@gmail.com** including the following:

- a) An email dated on or about March 27, 2017 with no subject line, which contained in the body a link to the website privnote.com; your Affiant knows privnote.com to be a website that offers users the ability to send free confidential and self-destructing messages via email;
- i. During the course of this investigation, investigators interviewed a co-conspirator who referenced the use of privnote.com messages when corresponding with other co-conspirators;
- b) An email dated on or about June 26, 2017 with the subject line “FW: Corporate Filing – 000300312800” which contained in the body a forwarded email concerning the filing of Articles of Organization for ELEGANT BEAUTY PRODUCTS LLC on or about June 13, 2017;

moderneffectscalls@gmail.com

- 58. Records obtained from Google, Inc. show the email address **moderneffectscalls@gmail.com** was created on or about June 26, 2017 and the listed recovery email is **moderneffectsdetroit@gmail.com**;
- 59. The email address **moderneffectscalls@gmail.com** received over 1,600 emails from an email address associated with the website ringboost.com; all of these emails were also received into the email inbox of **timlee5454@gmail.com** and included the following:
 - a) An email sent on or about August 31, 2017 with the subject line “Call Notification | 700-519-3770, 866-355-3229 | Sent to: 808-446-5435 | Duration: 00:00:51” was sent from **callreporting@ringboost.com** and included the caller ID information for telephone number 217-632-XXXX associated with an individual hereinafter referred to as Person – JD;
 - i. Records obtained from SunTrust Bank show on or about August 31, 2017 a wire transfer totaling \$12,900 was sent from an Independent Banker’s Bank account associated with Person – JD and received by a SunTrust Bank account ending in #4877 associated with the business name EASY BUSINESS PARTNERS LLC;
 - b) An email sent on or about September 27, 2017 with the subject line “Call Notification | 700-519-3770, 866-355-3229 | Sent to: 808-446-5435 | Duration: 00:01:07” was sent from **callreporting@ringboost.com** and included the caller ID information for telephone number 901-490-XXXX associated with an individual hereinafter referred to as Person – SW;

- i. Records obtained from Regions Bank show on or about September 27, 2017 a wire transfer totaling \$8,000 was sent from a Bank of America bank account associated with Person – SW and received by a Regions Bank account ending in #1461 associated with the business name ELEGANT BEAUTY PRODUCTS LLC;

elegantbeautyproductsmia@gmail.com

60. Records obtained from Google show the email address **elegantbeautyproductsmia@gmail.com** was created on or about June 13, 2017 and was logged into as recently as on or about December 12, 2017; The recovery email listed for this email address is **moderneffectsdetroit@gmail.com**;
61. The email address **elegantbeautyproductsmia@gmail.com** sent at least one email to the email address **timlee5454@gmail.com** as follows:
 - a) An email dated on or about June 16, 2017 with no subject line which contained in the body a link to the website privnote.com;
 - b) As referenced above an email was sent on or about June 26, 2017 from **prepaidcustomer18@gmail.com** to **timlee5454@gmail.com** which contained Articles of Organization for ELEGANT BEAUTY PRODUCTS LLC;
62. Bank records obtained from Regions Bank show an account ending in #1461 was opened in the name ELEGANT BEAUTY PRODUCTS LLC; in or around September 2017 this account received five wire transfer deposits totaling approximately \$65,200. These wires reference “EBP” and one specifically references an eBay invoice number and a John Deere vehicle;

moderneffectsdetroit@gmail.com

63. Records obtained from Google, Inc. show the email address **moderneffectsdetroit@gmail.com** was created on or about March 7, 2017 and was logged into as recently as on or about December 4, 2017;
64. The email address **moderneffectsdetroit@gmail.com** sent at least one email to the email address **timlee5454@gmail.com** as follows:
 - a) An email on or about June 20, 2017 with no subject line that contained in the body a link to a privnote.com message; as noted above this is a service that provides free confidential and self-destructing messaging;

65. As referenced above documents obtained from Google, Inc. show the email address **moderneffectsdetroit@gmail.com** was listed as the recovery email address for the email addresses **moderneffectscalls@gmail.com** and **elegantbeautyproductsmia@gmail.com**;

godaffiliated@gmail.com

66. Records obtained from Google, Inc. show the email address **godaffiliated@gmail.com** was created on or about March 29, 2013 and was logged into as recently as on or about July 12, 2018;

67. The email address **godaffiliated@gmail.com** sent at least one email to the email address **timlee5454@gmail.com** as follows:

- a) An email dated on or about February 22, 2017 with the subject line "aaron" that contained in the body of the email several images including a credit report, credit score and profile for an individual hereinafter referred to as "Person – AN."
- i. An individual hereinafter referred to as Person – KS filed a complaint with law enforcement stating on or about August 8, 2018 Person – KS attempted to purchase a John Deere vehicle through eBay and was instructed to send payment totaling \$22,000 via wire to a Fifth Third Bank account held in the name Person – AN; Person – KS did not receive the vehicle in question;
- ii. An individual hereinafter referred to as Person – FP filed a complaint with law enforcement stating Person – FP attempted to purchase a boat through eBay and was instructed to send payment totaling \$22,900 via wire to a SunTrust Bank account held in the name of Person – AN; Person – FP did not receive the vehicle in question;

reneeorb@gmail.com

68. Records obtained from Google, Inc. show the email address **reneeorb@gmail.com** was created on or about March 4, 2013 and was logged into as recently as on or about July 5, 2018;

69. The email address **reneeorb@gmail.com** received at least two emails from the email address **farmerjohn0915@gmail.com** as follows:

- a) An email dated on or about December 4, 2015 with the subject line "Fwd: Tattoos info"

which contained in the body bank account information for a business named ENTERPRISE BUSINESS PLANNING LLC. Your affiant knows the name "Tattoo" to be a nickname used by an individual involved in the fraud scheme;

- b) An email dated on or about December 4, 2015 with the subject line "Fwd: Tattoo pic and I update the sheet" which contained in the body a forwarded email with multiple images of bank checks and bank account opening documents;

70. Bank records obtained from JPMorgan Chase bank show the email address **reneeorb@gmail.com** is associated with Shalitha Schexnayder and the business ORIXA LLC;

- a) Multiple emails were received by the email address **elmasboutiquepa@gmail.com** from the email address **donotreply@billing-notification.com** referencing payments made to ORIXA LLC;

- i. Investigators have identified Elma's Boutique Personal Assistants as one of the business entities established for use in the fraud scheme. Multiple bank accounts have been identified including two accounts held at Regions Bank which received five wire transfers totaling approximately \$58,740.

- b) On or about March 17, 2017 an email was sent from the email address **prepaidcustomer18@gmail.com** to the email address **ecommercebusinesspioneers@gmail.com** with no subject line and in the body listed the business name ORIXA LLC and an address in Aventura, FL;

- i. Investigators have identified Ecommerce Business Pioneers as one of the business entities established for use in the fraud scheme. Multiple bank accounts have been identified including two accounts held at Regions Bank that received six wire transfers totaling approximately \$74,000.

s.g.chickey@sudenllinks.net

71. Records obtained from Google show the email address **s.g.chickey@sudenllinks.net** was created on or about September 15, 2017 and was logged into as recently as November 7, 2017;

72. The email address **s.g.chickey@sudenllinks.net** sent at least one email to the email address **jimmypang44@gmail.com** as follows:

- a) An email sent on or about October 27, 2017 with the subject line “Fwd: Fwd: Wire request completed” which contained in the body a twice forwarded email originally sent from Charles Schwab and Co Inc. detailing a wire transfer totaling \$12,000 sent from a Charles Schwab account ending in #747 to a TD Bank account ending in #891; the listed wire recipient was “EBPA”;
 - i. Records obtained from TD Bank show an account ending in #891 was opened in the business name EXTRAORDINARY BUSINESS PRODUCTS & APPLICATIONS LLC and received a wire transfer of \$12,000 from a Charles Schwab bank account on or about October 27, 2017;
73. There is probable cause to believe that there are records and other items, as set forth in Attachment B, Section II, located in the following email accounts:

jimmytang44@gmail.com
timmywang9898@gmail.com
timlee5454@gmail.com

denise.raymond67@gmail.com
galeaua@gmail.com
cardsg4@gmail.com
payme0181@gmail.com
bshireley@gmail.com
holly.toner83@gmail.com
vanessawilliams870@gmail.com
toddrichman1@gmail.com
prepaidcustomer18@gmail.com
moderneffectscalls@gmail.com
elegantbeautyproductsmia@gmail.com
moderneffectsdetroit@gmail.com
godaffiliated@gmail.com
reneeorb@gmail.com
s.g.chickey@sudenllinks.net

as set forth in Attachment B, Section I, which contain evidence relating to criminal activity.

TECHNICAL BACKGROUND

74. In order to ensure that agents search only the computer accounts and/or files described in Attachment B, this affidavit and application for a search warrant seek authorization to permit employees of the Service Providers to assist agents in the execution of this warrant. The search warrant will be transmitted electronically to the Service Providers' personnel who will be directed to produce the information described in Attachment B.
75. Based on my training and experience, the training and experience of other special agents, and information conveyed to me by persons knowledgeable in computer forensics, I have learned that Google, Inc. provides a variety of online services, including electronic mail ("email") access, to the general public. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, email transaction information, and account application information.
76. In general, an email that is sent to a Google, Inc. subscriber is stored in the subscriber's "mailbox" on Google, Inc. servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, Inc. servers indefinitely.
77. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google Inc.'s servers, and then transmitted to its end destination. Google, Inc. often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google, Inc. server, the email can remain on the system indefinitely.
78. A Google, Inc. subscriber can also store files, including emails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Google, Inc.
79. Subscribers to Google, Inc. might not store on their home computers copies of the emails stored in their Google, Inc. account. This is particularly true when they access their Google, Inc. account through the web, or if they do not wish to maintain particular emails or files in their residence.
80. In general, email providers like Google, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

81. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google, Inc.'s website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.
82. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

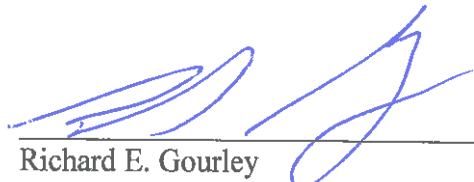
SUMMARY

83. Based on your affiant's training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Google, Inc. there exists evidence of criminal activity. Accordingly, a search warrant is requested.
84. This Court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation," pursuant to 18 U.S.C. § 2703(a).
85. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST TO SEAL

87. The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), Google, Inc. be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.
88. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. Your affiant believes that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal activity which may later involve additional individuals. Based upon my training and experience, your affiant has learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness. Wherefore, for all the foregoing reasons, the government requests that all files related to the search warrant issued in his case, including the search warrant application and affidavit in support thereof, be sealed.

FURTHER AFFIANT SAYETH NAUGHT.


Richard E. Gourley
Special Agent, IRS-CI

Subscribed to and sworn before me this 12 day of October, 2018.


HONORABLE CHELSEY M. VASCURA
UNITED STATES MAGISTRATE JUDGE

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

**IN THE MATTER OF
THE SEARCH OF:**

NO. _____

**jimmypang44@gmail.com
timmywang9898@gmail.com
timlee5454@gmail.com**

**denise.raymond67@gmail.com
galeaua@gmail.com
cardsg4@gmail.com
payme0181@gmail.com
bshireley@gmail.com
holly.toner83@gmail.com
vanessawilliams870@gmail.com
toddrichman1@gmail.com
prepaidcustomer18@gmail.com
moderneffectscalls@gmail.com
elegantbeautyproductsmia@gmail.com
moderneffectsdetroit@gmail.com
godaffiliated@gmail.com
reneeorb@gmail.com
s.g.chickey@sudenllinks.net**

**Google, Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043**

ATTACHMENT A: PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following Google, Inc. e-mail accounts:

**jimmypang44@gmail.com
timmywang9898@gmail.com
timlee5454@gmail.com**

**denise.raymond67@gmail.com
galeaua@gmail.com**

cardsg4@gmail.com
payme0181@gmail.com
bshireley@gmail.com
holly.toner83@gmail.com
vanessawilliams870@gmail.com
toddrichman1@gmail.com
prepaidcustomer18@gmail.com
moderneffectscalls@gmail.com
elegantbeautyproductsmia@gmail.com
moderneffectsdetroit@gmail.com
godaffiliated@gmail.com
reneeorb@gmail.com
s.g.chickey@sudenllinks.net

that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF
THE SEARCH OF:

NO. _____

jimmypang44@gmail.com
timmywang9898@gmail.com
timlee5454@gmail.com

denise.raymond67@gmail.com
galeaua@gmail.com
cardsg4@gmail.com
payme0181@gmail.com
bshireley@gmail.com
holly.toner83@gmail.com
vanessawilliams870@gmail.com
toddrichman1@gmail.com
moderneffectscalls@gmail.com
elegantbeautyproductsmia@gmail.com
moderneffectsdetroit@gmail.com
prepaidcustomer18@gmail.com
godaffilaite@gmail.com
reneeorb@gmail.com
s.g.chickey@sudenllinks.net

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043

ATTACHMENT B: ITEMS TO BE SEIZED

Section I

Information to be disclosed by Google, Inc.:

To the extent that the information described in Attachment A is in the possession, custody, or control of Google, Inc., regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs or information that has been deleted but is still available to Google, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between Google, Inc. and any person regarding the account, including contacts with support services and records of actions taken; and
- f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored;

Google, Inc. is hereby ordered to disclose the information to the government within fourteen days of the issuance of this warrant.

Section II

Information to be seized by the government:

All information described above in Section I that constitutes fruits, evidence, and/or instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1956 (money laundering), and/or 18 U.S.C. § 371 (conspiracy), those violations involving Terry Boutwell, Tiffany Strobl, and others, and occurring on or after the periods as detailed below, including, for each account identifier listed on Attachment A, information pertaining to the following matters:

Search Periods as follows:

jimmytang44@gmail.com – December 1, 2017 to the present

timmywang9898@gmail.com – May 1, 2017 to the present

timlee5454@gmail.com – December 1, 2017 to the present

denise.raymond67@gmail.com – February 1, 2017 to the present

galeaua@gmail.com – April 1, 2015 to the present

cardsg4@gmail.com – February 1, 2017 to the present

payme0181@gmail.com – January 1, 2017 to the present

bshireley@gmail.com – September 1, 2016 to the present

holly.toner83@gmail.com – June 1, 2016 to the present

vanessawilliams870@gmail.com – September 1, 2016 to the present

toddrichman1@gmail.com – November 1, 2016 to the present

prepaidcustomer18@gmail.com – June 1, 2016 to the present

moderneffectscalls@gmail.com - June 1, 2017 to the present

elegantbeautyproductsmia@gmail.com – June 1, 2017 to the present

moderneffectsdtroit@gmail.com – March 1, 2017 to the present

godaffiliated@gmail.com – April 1, 2015 to the present

reneeorb@gmail.com – April 1, 2015 to the present

s.g.chickey@sudenllinks.net – September 1, 2017 to the present

- a. Evidence containing the following names or aliases in whole or part or any variation or derivatives of such names: Terry Boutwell, Tiffany Strobl, Bob, Ghost, Rambo, Melissa Ramsey, Kaylee Lieninger, Scott Brownell, Alex, Ashley Robbins, Rebecca Dawson, Karen Burke, Jessica Thomey, Kim Young, Bibz, Monk, eBay, eBay Buyer Protection, EBPA, EEBPA, EEBP, EBMP Associates, EBMP Services, Enison Business Protection Advisors, Ecommerce Business Protocol Architects, Evil Boy Productions, and/or any other business names containing any combination of the letters EBP.
- b. Evidence referencing or regarding online marketplaces such as Craigslist and eBay.
- c. Evidence regarding or referencing the purchase, sale or exchange of motor vehicles and/or virtual currency such as Bitcoins including advertisements, inquiries, contracts, invoices, financing, payment, and delivery of goods.
- d. Evidence referencing or regarding banks, banking transactions, and/or the movement of funds including the opening and closing of bank accounts; deposit, transfer and withdrawal activity; the purchase or negotiation of checks; credit card transactions; account balances; returned items; fraud notices; transaction notices; receipts and statements.

- e. Evidence referencing or regarding dollar amounts and percentages.
- f. Evidence referencing or regarding a “tally;”
- g. All communications with, between or regarding any of the following email accounts:

jimmypang44@gmail.com
timmywang9898@gmail.com
timlee5454@gmail.com

denise.raymond67@gmail.com
galeaua@gmail.com
cardsg4@gmail.com
payme0181@gmail.com
bshireley@gmail.com
holly.toner83@gmail.com
vanessawilliams870@gmail.com
toddrichman1@gmail.com
prepaidcustomer18@gmail.com
moderneffectscalls@gmail.com
elegantbeautyproductsmia@gmail.com
moderneffectsdetroit@gmail.com
godaffiliated@gmail.com
reneeorb@gmail.com
s.g.chickey@sudenllinks.net

- h. Evidence referencing or regarding the opening, closing, access, control or use of any email accounts.
- i. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- j. Evidence referencing or regarding cell phone and/or toll free telephone number services including the opening, closing, use or control of service accounts; applications for service; assignment of telephone numbers; contracts; invoices; statements and receipts; Google Voice accounts; text messages or voicemails;
- k. Evidence referencing or regarding the establishment, organization, operation and/or control of businesses.

- l. Evidence containing, referencing or regarding personal identification information including names, dates of birth, addresses, phone numbers, social security numbers, driver's license numbers, and/or employer identification numbers.
- m. Evidence containing, referencing or regarding usernames and/or passwords.
- n. Evidence referencing or regarding travel including rental cars, flights, hotel reservations, travel directions, confirmation numbers, contracts, invoices and receipts.
- o. Evidence referencing or regarding eBay, eBay Buyer Protection or escrow services.
- p. Evidence providing information regarding the identities of any person(s) who created, used, accessed and/or exercised control over the account in question and/or the time/location from which such control was exercised, including records that help reveal the whereabouts of such person(s);